National Priority 3: Implement the National Infrastructure Protection Plan (NIPP)

The statewide program manager for this effort is:
Mike McAllister
Office of Commonwealth Preparedness
804-692-
Mike.mcallister@governor.virginia.gov

For questions on this section please contact Mike.

To provide input on any part of this section please direct your comments to:
Susan Mongold
Office of Commonwealth Preparedness
804-692-2598
Susan.mongold@governor.virginia.gov

This section should address the Critical Infrastructure Protection Program as defined below:

- In accordance with the risk management framework (RMF) identified in the NIPP and benchmarks identified in the FY 2006 and 2007 HSGP Grant Guidance, does the State have a critical infrastructure and key resource (CI/KR) protection program as a component of their overarching homeland security program? If so, please describe how the program supports the RMF identified in the NIPP according to the following six areas of the RMF.
  - **Set Security Goals.** How has the program been structured to define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture? Please include any information about the program's governance structure, participating entities/stakeholders, advisory groups, or other partnerships at the Federal, State, and local levels, and public/private sector outreach activities.
  - **Identify Assets, Systems, Networks, and Functions.** Describe how the program conducts an inventory of the assets, systems, and networks, including any Information Technology (IT) and Geographic Information Systems (GIS) tools, databases, and/or systems that support the collection, storage, and/or management of this information.
  - **Assess Risks.** Describe how the program determines and/or assesses risk, as a function of consequences, vulnerabilities, and threats. Please include information on the processes, tools, and/or methodologies used to conduct risk assessments, or any partnerships that support these efforts (i.e., fusion centers and PSAs).
  - **Prioritize.** Describe what processes, programs, and/or tools are leveraged by the program to aggregate and analyze risk assessment results, establish priorities based on risk, and determine protection and business continuity initiatives that provide the greatest mitigation of risk.
  - **Implement Protective Programs.** Describe how the program reduces and/or manages identified risks through the implementation of protective programs. Please include how the program identifies and obtains resources (both Federal and non-Federal) to address priorities and how the protective programs are coordinated with other Federal, State, and local partners (i.e., Fusion Centers, PSAs, RTSWGs, AMSCs, etc).
  - **Measure Effectiveness.** How does the program use metrics and other evaluation procedures to measure progress and assess the effectiveness of the CI/KR protection efforts in improving protection, managing risk, and increasing resiliency?

Describe what the State has done to pursue PCII accreditation to enable State government and attending local government agencies to access PCII. Accreditation activities may include signing an MOA with DHS, appointing a PCII Officer, training potential and current PCII users, and implementing a self-inspection.

National Priority 3: Implement the National Infrastructure Protection Plan (NIPP)

A. Accomplishments

Analysis of DHS Critical Infrastructure (CI) Sites
Working closely with Office of Commonwealth Preparedness, the Virginia Department of Transportation controls Virginia's critical infrastructure program. Thus far, Virginia has completed an analysis of sites identified by DHS as critical infrastructure and has developed its own list of Critical Infrastructure that is currently being refined by the Resiliency Study (discussed below).

Working with the Private Sector
There are currently over 20,000 Critical Infrastructure/Key Resource (CI/KR) sites in Virginia, approximately 85 percent of which are owned and operated by the private sector. As such, collaboration with the private sector has been a primary focus for Virginia when striving to implement the NIPP throughout the Commonwealth.

Through the fusion center, EOC, and critical infrastructure outreach efforts, Virginia is partnering with utility companies to deter threats to vital infrastructure and enhance coordination of prevention and preparedness initiatives between local and State government and the utility industry.

Automated Critical Asset Management System (ACAMS)
Constellation/Automated Critical Asset Management System is a web-based tool managed by DHS to collect information on critical assets, compile data, assist with vulnerability assessments, and generate a variety of reports. The Virginia Governor's Office of Commonwealth Preparedness is deploying ACAMS to promote regional collaboration. It will be locally managed (with support provided by DHS and the Virginia Fusion Center) and will become Virginia's fundamental recording tool on critical infrastructure as the Commonwealth switches over from IMAP.

Protected Critical Infrastructure Information (PCII) Program
Virginia has completed the necessary initial requirements, and is now awaiting accreditation from the DHS PCII Program Office as well as approval from the Virginia Office of Commonwealth Preparedness and the Attorney General.

Port Security
The AMS port security plans have been developed under the aegis of the appropriate U. S. Coast Guard Captain of the Port and provide integrated, layered defense for Virginia's ports. These plans coordinate Coast Guard and Navy as well as private, local and State security and law enforcement, assets in an integrated and cooperative protection program. Additionally, the

Governor's office is represented on both the Baltimore and Hampton Roads Maritime Commissions, helping ensure these plans are carefully coordinated.

Airport Security
Virginia has invested in the Department of Aviation including funding training, establishing standards and inspections, creating a database of pilots and planes, and doing awareness work with airport operators and owners through their respective associations.

DOAV is providing oversight of the General Aviation Security Program and coordinating with airport sponsors to improve compliance with current aviation security practices. DOAV established the Virginia Airports Security Advisory Committee (VASAC) to develop improved security measures and to advise the Commonwealth on General Aviation security-related matters.

Training
Virginia has completed 100% of its established milestones for CI training. The Commonwealth requires Terrorism Awareness training of all State employees and has been working to supply private industry with soft target awareness training. The Commonwealth has also developed and distributed instruction manuals and templates describing how to conduct and prepare general aviation Airport Security Audits/Plans

Equipment
In preparation for the Jamestown 400th Celebration, cameras, jersey barriers, sensors, communications equipment etc. were purchased. Virginia has also recently purchased security equipment for underwater security in Hampton Roads.

Virginia is the focus of a pilot project with the Domestic Nuclear Detection Office (DNDO) where a radiological detector was installed in the Stephen City weigh-station and a portable detector placed on I-81.

B. Current Capabilities

Critical Infrastructure Protection Program:

- State CIP plans are in place.
- Appropriate risk methodology has been developed, and information has been collected about assets, systems, networks, and functions relevant to this effort.
- Sector-specific agencies have identified assets of potential regional importance.
- A mechanism for coordinating CIP efforts is in place.
- Sector security goals support the goal of the NIPP.
- Risk assessment training program is developed and implemented.
- Data has been collected on assets, systems, networks, and functions and address dependencies and interdependencies that affect functionality and performance.
- Consequence or “top-screen” analysis has been performed.
- Potential threats to assets, systems, networks, and functions have been identified.
- Risk analysis results were disseminated to the proper authorities.

C. Three-Year Targets

Critical Infrastructure Protection Program:

Target Description	Projected Completion Year	Status
To implement the Commonwealth's Critical Infrastructure Protection and Resiliency Strategic Plan focused the State, regional, and local efforts for infrastructure protection.	2010	Open
Conduct regional, sector analysis of CI/KR to establish risk, interdependencies and a baseline for resiliency.	2010	Open
Determine which agencies and employees (State and local) need training prior to DHS's PAS system becoming operable. Conduct this training using the best format available.	2010	Open
Development of a PCII website which will contain information on the Virginia CII Code, SOP, CII Act, SSI Federal Regulations, Federal Register, and PCII Work Product Guide	2010	Open
Implement a statewide technological security structure through the Commonwealth IT Security Program	2010	Open
Establish collaborative plans, equipment, training, and protection standards for security of transportation systems to include surface, aviation, and seaports.	2010	Open
Establish plans, procedures, training, and exercises necessary to protect facilities providing water, power, and communications.	2010	Open

D. Initiatives

Critical Infrastructure Protection Program:

Implement the National Infrastructure Protection Plan in the Commonwealth of Virginia through development of sector specific working groups and an analysis of the critical infrastructures/key resources within each region. (Targets 1, 2, 3, 6, 7)

Description:
This Initiative will support the implementation of the National Infrastructure Protection Plan (NIPP) and strives to achieve the goals and objectives set forth in the Secure Commonwealth Initiative Strategic Plan. The following areas in particular are critical to implementation of the NIPP:

Plan Development

- The homeland security regions will develop regional plans to support preparedness and response initiatives. Each region's plan should include profiles of infrastructure, critical facilities, and resources to support operations.
- An aggressive plan will be developed to conduct standardized risk and vulnerability assessments for critical infrastructure training to local law enforcement and CI/KR sector representatives.

Key Personnel and Partnerships

- The employment of a statewide Critical Infrastructure Protection Coordinator and seven Regional Infrastructure Security Coordinators will support the management of the statewide and regional implementation of the program.
- Existing working groups, community organizations, and government personnel will help harden all CI/KR facilities within the Commonwealth.
- State and local governments will partner with the private sector and utilities to enhance initiatives to deter threats to vital infrastructure.
- State and local governments will implement a public awareness program promoting citizen and private sector protection of critical transportation infrastructure.

Resiliency Study

- While Virginia has completed a macro-level examination of statewide critical infrastructure, Hampton Roads is the first region to conduct an in-depth resiliency study to identify preparedness gaps and interdependencies. This project will be complete in 2008. Virginia plans to conduct similar studies in other regions to get an overarching picture for the entire Commonwealth, and the NCR is planning a similar project using funds from the 2007 NCR UASI grant.

Geographic Scope:

This Initiative will cover the implementation of the National Infrastructure Protection Plan in all seven homeland security regions and will encompass all seventeen sectors of Critical Infrastructure and Key Resources as identified by the Department of Homeland Security. The risk and vulnerability assessment training portion of the Initiative will be focused on local entities. It will impact each of the Commonwealth's jurisdictions and the entire Commonwealth's population of over 7 million citizens.

Program Management:

It is currently led by the VDOT Security Division and the Office of Commonwealth Preparedness with the advice and coordination from the SCP and CPWG Sub-Panel. Private Industry, such as Dominion Power and Verizon, has also played a key role in the establishment of the NIPP. OCP serves as the coordinating body for all of these groups.

Apply technology and security standards to the implementation of the NIPP in the Commonwealth of Virginia (Targets 4, 5, 6, 7)

Databases

- Develop a PSCII compliant website for management of all CI/KR data
- The Commonwealth will continue to use the ACAMS to document critical transportation infrastructure and key assets. Stakeholders coordinate use of this data to develop a written plan to safeguard these assets and infrastructure, such as the enforcement of maritime exclusion zones.
- Continue to update the assets list through "Data Call", an annual updating process for the NADB. This system maintains a listing of every potential critical asset (20,000) in the Commonwealth.
- Continue to update the BZPP for Virginia assets.
- Continue to train users who access ACAMS and other secure programs.

Training and Exercises

- Develop and deliver risk and vulnerability assessment training to local law enforcement and emergency management agencies across the Commonwealth. Through this training, 5-person Risk and Vulnerability Assessment Teams will be formed within each of the Commonwealth's 134 localities. These teams will perform comprehensive all-hazards risk and vulnerability assessments at designated CI/KR sites.
- Coordinate with the HSEEP training and exercise program the use of CI/KR data, databases, and training to apply NIPP into routine prevention and recovery planning.

Geographic Scope:
This Initiative will cover the implementation of the National Infrastructure Protection Plan in all seven homeland security regions and will encompass all seventeen sectors of Critical Infrastructure and Key Resources as identified by the Department of Homeland Security. The risk and vulnerability assessment training portion of the Initiative will be focused on local entities.

Program Management:
It is currently led by the VDOT Security Division and the Office of Commonwealth Preparedness with the advice and coordination from the SCP and CPWG Sub-Panel. Private Industry, such as Dominion Power and Verizon, has also played a key role in the establishment of the NIPP. OCP serves as the coordinating body for all of these groups.

E. Resources

Resources Expended in FY 2007

The NIPP is being implemented throughout the Commonwealth but Homeland Security grant funds are not being used. Currently state funds and Federal Highway Administration funds have been used for NIPP implementation. Furthermore the Buffer Zone Protection Program is managed by VDOT.

Critical Infrastructure/Key Resources Protection Program – This 2007 investment supports the First Responder Authentication Credential smart cards now issued to employees and contractors in Northern Virginia and the Hampton Roads area. It also provides training on the

Automated Critical Asset Management System for more than 300 local law enforcement officers. **$1,227,750**

Future Resources Required

To complete implementation of the NIPP, resources are needed as follows:

Seven regional CI coordinators (7 positions for three years)	$ 1,600,000
ACAMS training (5 persons in 134 localities)	$ 1,000,000
Resiliency studies of remaining six regions (1 region was $1.7m)	$ 9,000,000
Equipment for hardening	$ 3,000,000
Website security, support, standards	$ 500,000
Total resources required 2007-2010	$14,500,000